Commentary

BIG DATA & SOCIETY

Big Data & Society
January–June 2017: 1–10

DOI: 10.1177/2053951717691550
journals.sagepub.com/home/bds
SAGE

Big Data is a big lie without little data: Humanistic intelligence as a human right

Steve Mann

Abstract

This article introduces an important concept: Transparency by way of Humanistic Intelligence as a human right, and in particular, Big/Little Data and Sur/Sous Veillance, where "Little Data" is to sousveillance (undersight) as "Big Data" is to surveillance (oversight). Veillance (Sur- and Sous-veillance) is a core concept not just in human–human interaction (e.g. people watching other people) but also in terms of Human–Computer Interaction. In this sense, veillance is the core of Human-in-the-loop Intelligence (Humanistic Intelligence rather than Artificial Intelligence), leading us to the concept of "Sousveillant Systems" which are forms of Human–Computer Interaction in which internal computational states are made visible to end users, allowing users (but not requiring them) to "jump" into the computational feedback loop whenever or wherever they want. An important special case of Sousveillant Systems is that of scientific exploration: not only is (big/little) data considered, but also due consideration must be given to how data is captured, understood, explored, and discovered, and in particular, to the use of scientific instruments to collect data and to make important new discoveries, and learn about the world. Science is a domain where bottom-up transparency is of the utmost importance, and scientists have the right and responsibility to be able to understand the instruments that they use to make their discoveries. Such instruments must be *sousveillant systems*!

Keywords

Transparency, Big Data, little data, surveillance, sousveillance, metaveillance, veillance, security, suicurity, sousveillance cultures, sousveillant assemblage, artificial intelligence, humanistic intelligence, privacy, priveillance

Introduction

Surveillance[1] (oversight, i.e. being watched) and sousveillance[2] (undersight, i.e. doing the watching) can both be thought of in the context of control theory and feedback loops.[3]

In particular, McStay considers surveillance in this way, i.e. in regard to the form of privacy that is inherently violated by profiling, and related closed-loop feedback systems that manipulate us while monitoring us (McStay, 2011). Ruppert considers the interplay between surveillance and public space, through a case study of Toronto's Dundas Square (Ruppert, 2006), where security guards prohibit the use of cameras while keeping the space under heavy camera surveillance. This surveillance without sousveillance (Mann, 2002a) creates a lack of integrity, i.e. surveillance is a half-truth without sousveillance (Mann et al., 2015).

The intersection of Sousveillance and Media was pioneered by Bakir, i.e. sousveillance as not merely a capture or memory right, but also sousveillance as a disseminational (free-speech) right. This gave rise to two important concepts: sousveillance cultures and sousveillant assemblage (Bakir, 2010), analogous to the "surveillant assemblage" of Haggerty and Ericson (2000).

Surveillance has strong connections to Big Data, where states and other large organizations, especially in law enforcement, collect data secretly, or at least

WearTech™ Humanistic Intelligence Foundation, Palo Alto, CA, USA

Corresponding author:
Steve Mann, Phenomenal ℝeality Lab™, 135 Churchill Avenue, Palo Alto, CA 94301, USA.
Email: mann@eecg.toronto.edu

maintain some degree of exclusivity in their access to the data (Newell, 2013).

Two important concepts have been proposed to help mitigate this one-sided nature of Big Data: (1) "giving Big Data a social intelligence" (Ruppert et al., 2015) and (2) the concept of "Personal Big Data" (Gurrin et al., 2014) which might more properly be called "little data". Both of these concepts embody Big Data's sensory counterpart that corresponds more to sousveillance than surveillance (Mann, 2016a).

The veillance divide is justice denied

A good number of recent neologisms like: "Big Data", "Internet of Things" ("IoT"), "Artificial Intelligence" ("AI"), etc., describe technologies that aim to grant the gift of sight, or other sensory intelligence, to inanimate objects. But at the same time these inanimate objects are being bestowed with sight, that very same sight (ability to see, understand, remember, and share what we see) is being taken away from humans. People are being forbidden from having the same sensory intelligence bestowed upon the things around them.

Indeed, we're surrounded by a rapidly increasing number of sensors (Cardwell, 2014) feeding often closed and secretive "Big Data" repositories (Pasquale, 2015). Entire cities are built with cameras in every streetlight (Miao, 2015; Spielman, 2015). Automatic doors, handwash faucets, and flush toilets that once used "single-pixel" sensors now use higher-resolution cameras and computer vision (Iott and Nelson, 2005) (and with time-of-flight camera in US20150268342; see also gesture-sensing shower, US20080256494).

Surveillance is also widely used without regard to genuine privacy, i.e. with only regard to Panoptic-privacy. In Alberta, for example, the Privacy Commissioner condones the use of surveillance cameras in the men's locker rooms of Calgary's Talisman Centre where people are naked (David Fraser, 2007) as long as only the police (or other "good people") can see the video. Westside recreation Centre also in Calgary, Alberta, also uses surveillance cameras in their men's (but not women's) locker rooms (Frakes, 2016) (Figure 1).

While surveillance (oversight) is increasing at an alarming rate, we're also seeing a prohibition on sousveillance (undersight).

Martha Payne, a 9-year-old student at a school in Scotland, was served disgusting school lunches that lacked nutritional value. So in 2012 she began photographing the food she was served (Payne and Payne, 2012). When she began sharing these photographs with others, she generated a tremendous amount of online discussion on the importance of good school nutrition. And she brought about massive improvements in the nutritional value of school lunches around the world. She also raised considerable money for charity, as a result of her documentary photography. But, in part

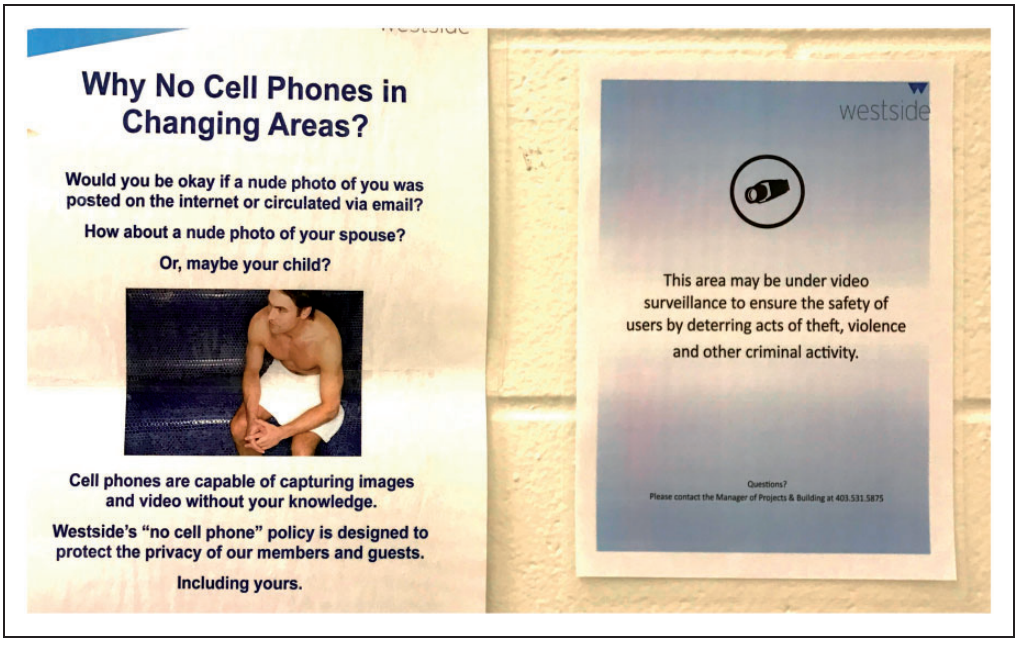

Figure 1. Westside Recreation Centre in Alberta, Canada, uses surveillance cameras in their men's (but not women's) shower/locker/changerooms (Edwardson, 2016), while they also have a "no cell phone" policy allegedly to "protect the privacy" of their guests.

due to the notoriety of her photo essays, she was suddenly banned from bringing a camera to school, and barred from photographing the lunches she was served by her school.

While schools begin the process of installing surveillance cameras, students are increasingly being forbidden from having their own cameras. And for many people on special diets, or with special health needs, using photography to monitor their dietary intake is a medical necessity. I proposed the use of wearable sensors (including wearable cameras) for automated dietary intake measurement in 2002 (US Pat. App. 20020198685; Mann, 2002c). This concept is now gaining widespread use for self-sensing and health monitoring (Doherty et al., 2013b, 2013a).

So when people suffer from acute effects like food poisoning or allergic reactions, or from longer-term chronic effects of poor nutrition, like obesity, being forbidden from keeping an accurate diary of what they have eaten is not just an affront to their free speech. It is also a direct attack on their health and safety.

Neil Harbisson, a colorblind artist and musician, has a wearable computer vision system that allows him to hear colors as musical tones. And he wears his camera and computer constantly. Wearable computing and Personal Imaging (wearable cameras) are established fields of research (Mann, 1997), dating back to my augmented reality vision systems of the 1970s. I also wear a computer vision system and visual memory aid. Harbisson and Mann both have cameras attached in such a way as to be regarded as part of their bodies, and thus their passports both include the apparatus, as it is a part of their true selves and likenesses (see Figure 2). And we are not alone: many people now are beginning to use technology to assist them in their daily lives, and in some ways, the transition from a surveillance society to a veillance society (i.e. one that includes both surveillance and sousveillance) is inevitable (Ali and Mann, 2013).

Referring back to Martha Payne, discussed earlier in this article, there is often an hypocrisy of the officials (schools, as well as society in general) wanting to collect more and more data about us, while forbidding us from collecting data about them or about ourselves (like monitoring our own dietary intake, monitoring our exercise, or helping us see and remember what we see). We need to be critical of this hypocrisy because (1) it is a direct threat to our health, wellness, and personal safety, and (2) data obtained under this hypocrisy lacks integrity (integrity is the opposite of hypocrisy). Thus it is with great joy and relief that we learn how Martha Payne fought back and won the right to continue using photography to monitor her dietary intake, not only for the journalistic freedom (in the Bakir sense), but also for the personal safety that such self-monitoring systems can provide.

Surveillance is a half-truth, without sousveillance

Surveillance is the veillance of hypocrisy, in the sense that, as often practiced by security guards, closely monitoring surveillance cameras, these guards tend to observe and object to individuals taking pictures in the surveilled spaces. The opposite of hypocrisy is integrity (Mann et al., 2015).

Surveillance typically tells a story from the side of the security forces. When stories told from other points-of-view are prohibited, i.e. the capturing of evidence to support these other points-of-view is prohibited, the total captured evidence is less than the full truth (Mann et al., 2015). In this sense, surveillance often gives rise to a half-truth.

Justeveillance (fair sight) in AI and machine learning

Much has been written about equiveillance, i.e. the right to record while being recorded (Manders, 2013; Mann et al., 2006; Weber, 2010, 2012a), and Martha's case is like so many others.

In the context of human–human interaction, the transition from surveillance to veillance represents a "fair" (French "Juste") sight and, more generally, fair and balanced sensing.

But our society is embracing a new kind of entity, brought on by AI (Artificial Intelligence) and machine learning. Whether we consider an "AI" as a social entity/actor, e.g. through Actor Network Theory (Callon, 1999; Latour, 2005; Munro, 2009; Wood and Graham, 2006), or simply as a device to interact with, there arises the question: "Are smart things making us stupid?" (Morozov, 2013).

Past technologies were transparent, e.g. electronic valves ("vacuum tubes") were typically housed in transparent glass envelopes, into which we could look to see all of their internals revealed. And early devices included schematic diagrams and parts lists—efforts by the manufacturer to help end users understand how their products worked.

In the present day of computer chips and closed-source software, manufacturers take extra effort not to help people understand how things work, but to conceal functionality: (1) for secrecy; and (2) because they (sometimes incorrectly) assume that their users do not want to be bothered by detail, i.e. that their users are looking for an abstraction and actually want "bothersome" details hidden (Burrell, 2016; Mann, 2016b).

At the same time these technologies are being more concealing and secretive, they are also being equipped with sensory capacity, so that (in the Actor Network Theory (ANT) sense) these devices are evolving toward knowing more about us while revealing less about themselves (i.e. toward surveillance).

Our inability to understand our technological world, in part through secrecy actions taken by manufacturers, and in part through a general apathy, leads to the use of modern devices through magic, witchcraft-like rituals rather than science (Lynn Kaarst-Brown and Robey, 1999). This technopaganism (Stivers and Stirk, 2001) leads people to strange rituals rather than trying to understand how things work. General wisdom from our experts tell us to "reboot" and try again, rather than understand what went wrong when something failed (Robertson, 2011). But this very act of doing the same thing (e.g. rebooting) over and over again, expecting a different result is the very definition of insanity:

> "Insanity is doing the same thing, over and over again, but expecting different results." (Narcotics Anonymous, 1981)

In this sense, not only do modern technologies drive us insane, they actually require us to be insane in order to function properly in the technopagan world that is being forced upon us by manufacturers who conceal its workings.

I propose[4] as a solution, a prosthetic apparatus that embodies the insanity for us, so that we don't have to. I call this app "LUNATIC". LUNATIC is a virtual personal assistant. The user places a request to LUNATIC and it then "tries the same thing over and over again…" on behalf of the user so that the user does not need to himself or herself become insane. For example, when downloading files, LUNATIC starts multiple downloads of the same file, repeatedly, and notifies the user when the result is obtained. LUNATIC determines the optimum number of

Figure 2. Harbisson and Mann with passports depicting the physical reality of their bodies as partly computational, both examples of people who are part technological, through the use of camera-based computer vision as a seeing aid. The Veillance Divide (e.g. when surveillance is the only allowable veillance) renders such people under attack as "existential contraband"—contraband by their mere existence.

simultaneous downloads. Typically this number works out to 2 or 3. A single download often stalls, and the second one often completes before the first. If too many downloads of the same file are initiated, the system slows down. So LUNATIC uses machine learning to detect slowed connections and makes a best guess as to the optimum number of times to repeat the same tasks over and over again. This number is called the "optimum insanity", and is the level of insanity (number of repetitions) that leads to the most likely successful outcome.

At times the optimum insanity increases without bound, typically when websites or servers are unreliable or erratic. LUNATIC is not performing a denial of service attack, but, rather, a "demand for service". A side effect is that when large numbers of people use LUNATIC, erratic websites will experience massive download traffic, such that LUNATIC disincentivises insanity.

In this sense, LUNATIC is a temporary solution to technopagan insanity, and ultimately will hopefully become unnecessary, as we transition to the age of Sousveillant Systems.

Sousveillant systems

Humanistic Intelligence is defined as intelligence that arises by having the human being in the feedback loop of a computational process (Minsky et al., 2013).

Sousveillant Systems are systems that are designed to facilitate Humanistic Intelligence by making their state variables observable. In this way machines are "watching" us while allowing us to also "watch" them. See detailed description in Mann (2016a), a figure from which is excerpted here (Figure 3).

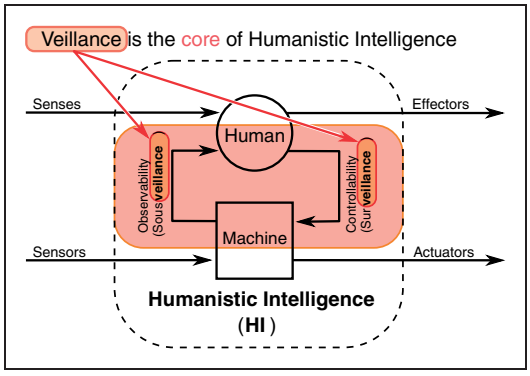

Figure 3. Humans have senses and effectors at their informatic inputs and outputs. Machines have sensors and actuators at their informatic inputs and outputs. The signal flow paths that connect them are surveillance (when we're being watched or sensed by the machine) and sousveillance (when we're watching or sensing the machine). Humanistic Intelligence (HI) requires all six of these signal flow paths to be present (Minsky et al., 2013). When one of the six is blocked (most commonly, Sousveillance), we have a breakdown in the feedback loop that allows for a true synergy ("cyborg" state). To prevent this breakdown, Sousveillant Systems mandate Observability (Sousveillance).

Cyborg craft

Sousveillant Systems give rise to a new form of Human–Computer interaction in which a machine can function as a true extension of the human mind and body. Manfred Clynes coined the term "cyborg" to denote such an interaction (Clynes and Kline, 1960), his favorite example being a person riding a bicycle (Clynes, 1996, personal communication). A bicycle is a machine that responds to us, and we respond to it in an immediate way. Unlike modern computers where feedback is delayed, a bicycle provides immediate feedback of its state variables all which can be sensed by the user.

Consider the Computer Numerical Control (CNC) milling machine that extends our capacity to make things. We begin with Computer Aided Design (CAD) and draw something, then send it to the machine, and let the machine work at it. There's not much real feedback happening here between the human and machine. The feedback is delayed by several minutes or several hours.

David Pye defines "craft" ("workmanship") as that which constantly puts the work at risk (Pye, 1968). As such, modern CNC machine work is not craft in the Pye sense. Nor is anything designed on a computer in which there is an "undo" or "edit revision history" functionality.

Imagine a CNC machine that gave the kind of feedback a bicycle does. Could we take an intimate experience in craft, like a potter's wheel, and make a CNC machine that works at that kind of continuous ("undigital") feedback timescale?

To answer this question, we are developing Haptic Augmented Reality Computer Aided Design (HARCAD) to create a new kind of craft called "Cyborg Craft" (see Figures 4 and 5).

Here we have a sensory synergy between human and machine, in which the feedback loop is essentially instantaneous.

Feedback delayed is feedback denied

Let us conclude with a hypothetical anecdote set in the future of musical instruments, which parallels the author's personal experience with scientific instruments. This points to a possible dystopia not so much of government surveillance, but of machine inequiveillance.

The year is 2067. Ken is the world's foremost concert pianist, bringing his own Steinway grand piano to each

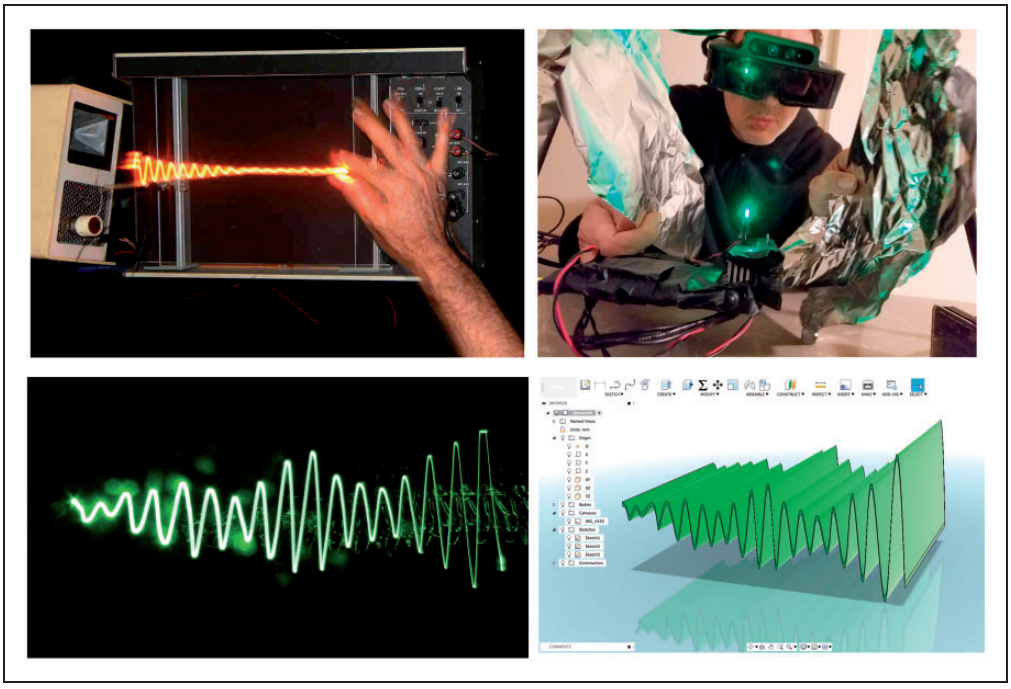

Figure 4. Haptics, Augmented Reality, and Computer Aided Design: A Tactile Sequential Wave Imprinting Machine (Mann, 2015, 1992) is formed from a linear actuator connected to an antenna moved in front of a radio transmitter (microwave motion sensor). The actuator is fed by a signal from a lock-in amplifier connected to the moving antenna plus another stationary antenna, so the user can grasp, touch, hold, and feel otherwise invisible electromagnetic radio waves. In an early embodiment (Mann, 1979), radio waves are picked up (or reflected) by the moving metal bar of a pen plotter, and the user grasps the pen to feel the radio waves. A light bulb is also attached to the pen so that the user can also see the radio waves, through Persistence-of-Exposure (PoE) of the human eye, or photographic film. In more modern embodiments, a linear actuator drives an LED light attached to the finger. By wrestling with this robotic device, the user and the device together trace out waves imported into the Autodesk Fusion 360 Cloud-Based 3D CAD Platform for instant collaboration with others. Together with the Metavision Augmented Reality glasses, multiple people use aluminum foil brushes to collaboratively sculpt and shape cloud-based metaveillance waveforms to design buildings, furniture, automobiles, or other curvaceous products.

concert he performs in, now that concert halls no longer have real pianos. Software synthesis has advanced to the point where none of the audience members can hear the difference. Steinway stopped making real pianos in 2020. Yamaha and others also switched to digital-only production the following year.

Even Ken has trouble telling the difference, when someone else is playing, but when he plays a real piano himself, he can feel the difference in the vibrations. In essence, the performance of the Steinway Digital is as good as the original, but the vibrotactile user-interface is delayed. The tactuators installed in each key simulate the player's feeling of a real piano, but there is a slight but noticeable delay that only the musician can feel. And user-interface is everything to a great musical performance.

Ken no longer has access to a real piano now that his Steinway grand piano was water-damaged by a roof leak while he was away last March. He tried to buy a new piano but could not find one. Tucker Music had one in their catalog, for $6,000,000, but when Ken called Jim Tucker, Jim said there were no more left. Jim sold about 50 of them at that price, over the past few years, as he collects and restores the world's last remaining real pianos, but no more are coming up for sale.

Ken has felt that his musical performances have declined now that he no longer has access to a real piano. Software, AI, and machine learning make better music anyway, so there's no longer a need for human musicians, anyway.

But there has been no great advancement in music in recent years, now that there are no longer any great musicians still passionate about music for music's sake. Today's musician spends most of the time writing grant proposals and configuring software license servers rather than playing music.

The need for antiques to obtain truth in science

The above story depicts a true event, except for a few small changes. My (not Ken's) instrument that was

Figure 5. Wrestling with robots as a means for achieving Cyborg Craft: Robotic-inspired abakographic light painting (top row). Stephanie, age 10, wrestles with the robot while controlling the spinning of a Potterycraft wheel with her left foot.

damaged was not a musical instrument, but, rather, a scientific instrument called a Lock-In Amplifier (Cosens, 1934; Meade, 1982; Michels and Curtis, 1941; Stutt, 1949) made by Princeton Applied Research in the early 1960s. It was easy to understand and modify. I actually did some modifications and parts-swapping among several amplifiers to get some special capabilities for AR (augmented reality) veillance visualizations, such as bug-sweeping and being able to see sound waves, radio waves, and sense sensors and their capacity to sense (Mann, 2015).

The roof leak occurred in March 2016, while the amplifier was running (it takes a few hours to warm up, and since it uses very little electricity it is best to leave it running continuously).

The PAR124A is no longer available, and large organizations like research universities and government labs are hanging on to the few that remain in operation.

It should be a simple matter of purchasing a new amplifier, but none of the manufacturers are willing to make the modifications I require, nor are they willing to disclose their principles of operation to allow me to do so. Neither Princeton Applied Research, nor Stanford Research Systems (nor any other modern maker of lock-in amplifiers) is able to supply me with an instrument I can understand.

One company claims to have equaled the performance of the PAR124A, at a selling price of $17,000:

> Since the invention of the lock-in amplifier, none has been more revered and trusted than the PAR124A by Princeton Applied Research. With over 50 years of experience, Signal Recovery (formerly Princeton Applied Research) introduces the 7124. The only lock-in amplifier that has an all analog front end separated, via fiber, from the DSP main unit.

Recent research findings, however, show that the PAR124A from the early 1960s still outperforms any scientific instrument currently manufactured (Wang et al., 2015).

And performance alone is not the only criterion. With a scientific instrument we must know the truth about the world around us. The instrument must function as a true extension of our mind and body, and hide nothing from us. Modern instruments conceal certain aspects of their functionality, thus requiring a certain degree of technopaganism (Stivers and Stirk, 2001) to operate.

Thus we currently live in a world where we can't do good science without access to antiques.

Imagine a world in which there are no Steinway grand pianos anymore, a world bereft of quality, except old ones in need of restoration. A musician would have to be or hire a restorer and repair technician, and hope for access to one of the few working specimens that remain.

Is this the world we want to live in?

Science demands integrity

Only through Sousveillant Systems and ''little data'' we can preserve the tradition of science, in the face of technopaganism, surveillance, and ''Big-only Data''. A goal of our research is to produce devices that embody sousveillance-by-design, starting with scientific test instruments like lock-in amplifiers, and progressing toward concepts like ''little data''. To that end, let us hope that we can build sousveillance into our networked world, starting with instruments.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. Lyon (2007); Norris et al. (2002).
2. Ali et al. (2013b, 2013a); Bakir (2010, 2009); Cardullo (2014); Fernback (2013); Fletcher et al. (2011); Ganascia (2010); Manders (2013); Mann (2002b); Mann et al. (2003); Mortensen (2014); Quessada (2010); Reilly (2015); Reynolds (2011); Vertegaal and Shell (2008); Weber (2012b).
3. Mann (2016a); Mann and Ferenbok (2013).
4. This began as an interventionist/awareness-raising effort, but could evolve into a useful field of research.

References

Ali MA, Ai T, Gill A, et al. (2013a) Comparametric HDR (High Dynamic Range) imaging for digital eye glass, wearable cameras, and sousveillance. In: *ISTAS*, IEEE, 27–29 June 2013, pp. 107–114.

Ali MA, Nachumow JP, Srigley JA, et al. (2013b) Measuring the effect of sousveillance in increasing socially desirable behaviour. In: *ISTAS*, IEEE, 27–29 June 2013, pp. 266–267.

Ali MA and Mann S (2013) The inevitability of the transition from a surveillance-society to a veillance-society: Moral and economic grounding for sousveillance. In: *ISTAS*, IEEE, 27–29 June 2013, pp. 243–254.

Bakir V (2009) Tele-technologies, control, and sousveillance: Saddam husseinde-deification and the beast. *Popular Communication* 7(1): 7–16.

Bakir V (2010) *Sousveillance, Media and Strategic Political Communication: Iraq, USA, UK*. London, UK: Continuum International Publishing Group.

Burrell J (2016) How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society* 3(1): 2053951715622512.

Callon M (1999) Actor-network theory the market test. *The Sociological Review* 47(S1): 181–195.

Cardullo P (2014) Sniffing the city: Issues of sousveillance in inner city London. *Visual Studies* 29(3): 285–293.

Cardwell D (2014) At Newark airport, the lights are on, and they're watching you. *New York Times*.

Clynes M and Kline N (1960) Cyborgs and space. *Astronautics* 14(9): 26–27, 74–75.

Cosens C (1934) A balance-detector for alternating-current bridges. *Proceedings of the Physical Society* 46(6): 818.

David Fraser P (2007) Cameras can stay in talisman's locker room, says commissioner. *CBC News* 22 March.

Doherty A, Williamson W, Hillsdon M, et al. (2013a) Influencing health-related behaviour with wearable cameras: Strategies & ethical considerations. In: *Proceedings of the 4th international sense cam & pervasive imaging conference*, ACM, 18–19 November 2013, pp. 60–67.

Doherty AR, Hodges SE, King AC, et al. (2013b) Wearable cameras in health. *American Journal of Preventive Medicine* 44(3): 320–323.

Edwardson L (2016) Westside recreation centre under fire for use of surveillance cameras in mens change room. *Calgary metro,* 3 October.

Fernback J (2013) Sousveillance: Communities of resistance to the surveillance environment. *Telematics and Informatics* 30(1): 11–21.

Fletcher G, Griffiths M and Kutar M (2011) A day in the digital life: A preliminary sousveillance study. *SSRN* Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1923629.

Frakes N (2016) Calgary REC centre reassures members after security breach. *CBC News,* 4 October.

Ganascia JG (2010) The generalized sousveillance society. *Social Science Information* 49(3): 489–507.

Gurrin C, Smeaton AF and Doherty AR (2014) Lifelogging: Personal big data. *Foundations and Trends in Information Retrieval* 8(1): 1–125.

Haggerty KD and Ericson RV (2000) The surveillant assemblage. *The British Journal of Sociology* 51(4): 605–622.

Iott J and Nelson A (2005) CCD camera element used as actuation detector for electric plumbing products. Canadian Patent 2602560; US and International patent application 11/105,900.

Latour B (2005) *Reassembling the Social: An Introduction to Actor-network-theory*. Oxford University Press.

Lynn Kaarst-Brown M and Robey D (1999) More on myth, magic and metaphor: Cultural insights into the management of information technology in organizations. *Information Technology & People* 12(2): 192–218.

Lyon D (2007) *Surveillance Studies An Overview*. Polity Press.

Manders C (2013) Moving surveillance techniques to sousveillance: Towards equiveillance using wearable computing. In: *ISTAS*, IEEE, 27–29 June 2013, pp. 19–19.

Mann S (1992) Wavelets and chirplets: Time–frequency perspectives, with applications. In: Archibald P (ed.) *Advances in Machine Vision, Strategies and Applications*. world scientific series in computer science. Vol. 32. Hong Kong: World Scientific.

Mann S (1997) Wearable computing: A first step toward personal imaging. *Computer* 30(2): 25–32.

Mann S (2002a) People watching people watchers: 'The law enforcement company' for watching over those who come to see and be seen on the 'urban beach'. *Surveillance & Society* 2(4): 594–610.

Mann S (2002b) Sousveillance, not just surveillance, in response to terrorism. *Metal and Flesh* 6(1): 1–8.

Mann WS (2002c) Slip and fall detector, method of evidence collection, and notice server, for usually impaired persons, or the like. Patent application 10/145,309, USA.

Mann S (2015) Phenomenal augmented reality: Advancing technology for the future of humanity. *IEEE Consumer Electronics* 4(4) cover +92–97.

Mann S (2016a) Surveillance (oversight), sousveillance (undersight), and metaveillance (seeing sight itself). In *Proceedings on IEEE CVPR (Computer Vision and Pattern Recognition), 2016 IEEE Conference*, Las Vegas, 26 June–1 July 2016, pp. 1408–1417. IEEE.

Mann S (2016b) Veillance integrity by design: A new mantra for CE devices and services. *IEEE Consumer Electronics* 5(1): 33–143.

Mann S and Ferenbok J (2013) New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society* 11(1/2): 18.

Mann S, Fung J and Lo R (2006) Cyborglogging with camera phones: Steps toward equiveillance. In: *Proceedings of the 14th annual ACM international conference on Multimedia*, ACM, 23–27 October, pp. 177–180.

Mann S, Janzen R, Ali MA, et al. (2015) Declaration of veillance (surveillance is half-truth). In: *Games entertainment media conference (GEM), 2015 IEEE*, IEEE, 14–16 October 2015, pp. 1–2.

Mann S, Nolan J and Wellman B (2003) Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society* 1(3): 331–355.

McStay A (2011) Profiling phorm: An autopoietic approach to the audience-as-commodity. *Surveillance & Society* 8(3): 310.

Meade M (1982) Advances in lock-in amplifiers. *Journal of Physics E: Scientific Instruments* 15(4): 395.

Miao W (2015) Method and system for transmitting video images using video cameras embedded in signal/street lights. U.S. Patent 9,202,358, issued 1 December 2015.

Michels WC and Curtis NL (1941) A pentode lock-in amplifier of high frequency selectivity. *Review of Scientific Instruments* 12(9): 444–447.

Minsky M, Kurzweil R and Mann S (2013) The society of intelligent veillance. In: *IEEE ISTAS 2013*, 27–29 June 2013.

Morozov E (2013) Is smart making us dumb. *The Wall Street Journal* Available at: https://www.wsj.com/articles/SB10001424127887324503204578318462215991802.

Mortensen M (2014) Who is surveilling whom? Negotiations of surveillance and sousveillance in relation to wikileaks release of the gun camera tape collateral murder. *Photographies* 7(1): 23–37.

Munro R (2009) Actor-network theory. *The SAGE handbook of power*. London: Sage Publications Ltd, pp. 125–139.

Newell BC (2013) Local law enforcement jumps on the big data bandwagon: Automated license plate recognition systems, information privacy, and access to government information. *Information Privacy, and Access to Government Information,* 16 October, 66.

Norris C, McCahill M and Wood D (2002) The growth of CCTV: A global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance & Society* 2(2/3): 110–135.

Pasquale F (2015) *The Black Box Society: The Secret Algorithms that Control Money and Information*. Harvard University Press.

Payne D and Payne M (2012) *NeverSeconds: The Incredible Story of Martha Payne*. Cargo Publishing.

Pye D (1968) *The Nature and Art of Workmanship*. Cambridge UP.

Quessada D (2010) De la sousveillance. *Multitudes* (1): 54–59.

Reilly P (2015) Every little helps? Youtube, sousveillance and the anti-tescoriot in stokes croft. *New Media & Society* 17(5): 755–771.

Reynolds C (2011) Negative sousveillance. In: *First international conference of the International Association for*

Computing and Philosophy (IACAP11), 4–6 July 2011, pp. 306–309.

Robertson V (2011) Deus ex machina? Witchcraft and the techno-world. *Literature & Aesthetics* 19(2): 279–306.

Ruppert E, Harvey P, Lury C, et al. (2015) Socialising big data: From concept to practice. CRESC working paper series (138).

Ruppert ES (2006) Rights to public space: Regulatory reconfigurations of liberty. *Urban Geography* 27(3): 271–292.

Spielman F (2015) Infrastructure Trust launches plan to overhaul Chicago's outdoor lights. *Chicago Sun-Times* 17 September.

Stivers R and Stirk P (2001) *Technology as Magic: The Triumph of the Irrational*. A&C Black.

Stutt CA (1949) Low-frequency spectrum of lock-in amplifiers. *Mit Technical Report No. 105*, 26 March 1949, pp 1–18. https://dspace.mit.edu/bitstream/handle/1721.1/4940/RLE-TR-105-04710621.pdf.

Vertegaal R and Shell JS (2008) Attentive user interfaces: The surveillance and sousveillance of gaze-aware objects. *Social Science Information* 47(3): 275–298.

Wang Y, Zhang Y, He X, et al. (2015) The signal detection technology of photoconductive detector with lock-in amplifier. In: *Selected proceedings of the photoelectronic technology committee conferences held on August–October 2014*, International Society for Optics and Photonics, pp. 95220F–95220F.

Weber K (2010) Mobile devices and a new understanding of presence. In: *12th ACM International Conference on Ubiquitous Computing UBICOMP2010*, Copenhagen, Denmark, 26–29 September 2010.

Weber K (2012a) Google glasses: Surveillance, sousveillance, equiveillance. In: *5th international conference on information law and ethics,* Corfu/Greece. Available at: papers.ssrn.com

Weber K (2012b) Surveillance, sousveillance, equiveillance: Google glasses. Social Science Research Network, Research Network Working Paper, pp. 1–3. Available at: http://tinyurl.com/6nh74jl

Wood D and Graham S (2006) Permeable boundaries in the software-sorted society: Surveillance and the differentiation of mobility. In: Sheller M and Urry J (eds) *Mobile technologies of the city*. London, UK: Routledge, pp. 177–191.

This commentary is a part of special theme on Veillance and Transparency. To see a full list of all articles in this special theme, please click here: http://bds.sagepub.com/content/veillance-and-transparency